(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－66592
（Ｐ2000－66592Ａ）
(43)公開日　平成12年３月３日(2000.3.3)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６５０	Ｃ０９Ｃ　1/00	６５０Ｂ	５Ｊ０４９
Ｇ０６Ｆ　7/58		Ｃ０６Ｆ　7/58	Ａ	
Ｈ０３Ｋ　3/84		Ｈ０３Ｋ　3/84	Ｚ	

審査請求　未請求　請求項の数5　ＯＬ　（全５頁）

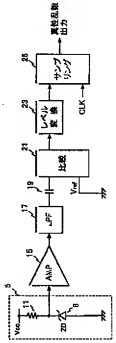
(21)出願番号　特願平10－232823
(22)出願日　平成10年８月19日(1998.8.19)

(71)出願人　596131492
システム工学株式会社
東京都千代田区神田錦町１－15－11
(71)出願人　396020800
科学技術振興事業団
埼玉県川口市本町４丁目１番８号
(72)発明者　長井　剛一郎
神奈川県相模原市御園３丁目２番７号
(74)代理人　100079119
弁理士　藤村　元彦

Ｆターム(参考)　5Ｊ049　AA00　AA14　AA15　BB01　CB01

(54)【発明の名称】　乱数生成装置

(57)【要約】
【目的】　暗号理論的に安全な２値乱数を容易に生成することが可能で、小型化に適した乱数生成装置を提供する。
【解決手段】　接合を含む半導体素子と、降伏電流が生じる程の逆バイアス電圧を接合に印加する逆バイアス印加手段と、接合を含む電流路に生ずる雑音信号をサンプリングして得られるデジタル信号を乱数として出力するデジタル化回路と、を有する。



【特許請求の範囲】
【請求項１】　接合を含む半導体素子と、降伏電流が生じる程の逆バイアス電圧を前記接合に印加する逆バイアス印加手段と、前記接合を含む電流路に生ずる雑音信号をサンプリングして得られるデジタル信号を乱数として出力するデジタル化回路と、からなることを特徴とする乱数生成装置。
【請求項２】　前記雑音信号の増幅信号を得る増幅回路と、
前記増幅信号を所定の基準電圧と比較して２値化信号を得る比較回路と、
前記２値化信号をサンプリングして、０及び１からなるサンプリング値系列を得るサンプリング回路と、を有することを特徴とする請求項１記載の乱数生成装置。
【請求項３】　前記半導体素子は、ツェナーダイオードであることを特徴とする請求項１又は２記載の乱数生成装置。
【請求項４】　前記サンプリング値系列における０及び１の各々の発生確率が略等しくなるように前記基準電圧を制御する制御手段を有することを特徴とする請求項２又は３記載の乱数生成装置。
【請求項５】　前記サンプリング値系列における０及び１の発生確率が略等しくなるように前記サンプリング値系列を平滑化する手段を有することを特徴とする請求項２又は３記載の乱数生成装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は乱数生成装置、特に、暗号化アルゴリズムに用いられる乱数生成装置に関する。
【０００２】
【従来の技術】インターネット、イントラネットの発展に伴い国際間取引、異業種取引、電子データ交換（ＥＤＩ：Electronic Data Interchange）などの新市場の開拓が盛んに行われている。一方、インターネットのオープン性から、ネットワーク上を往来する情報に対する不正行為（盗聴、改ざん、なりすまし、破壊行為等）への対応が必要であり、セキュリティ技術の開発が急がれている。
【０００３】ネットワークのセキュリティを確保するために広く暗号が利用されており、例えば、米国で標準化されているデジタル署名アルゴリズム（ＤＳＡ）がある。このような暗号化アルゴリズムにおいては、署名生成の度に乱数を生成させる必要があるが、用いる乱数としては「情報（暗号）理論的に安全な乱数」であることが望ましい。
【０００４】暗号理論的に安全な乱数とは、「乱数列の任意の一部から他のビットを多項式時間で推測できない」という条件を満たす乱数をいう。しかし、この条件はかなり厳しいので、実用上は以下のような評価尺度が用いられることがある。但し、これらはあくまでも必要条件に過ぎない。
（１）　０，１の等頻度性
（２）　長周期性
（３）　非線型性
（４）　線形複雑度が大きいこと
（５）　無相関性
非線型性というのは、乱数が線形フィードバックシフトレジスタ(linear feedback shift register)の出力そのものではないということである。ｎ段の線形フィードバックシフトレジスタで生成できる系列の最大周期は2^n-1であり、この周期2^n-1の系列をＭ系列(maximum length shift register sequence)と呼ぶ。従って、擬似乱数としてよく用いられるＭ系列はこの基準を満たしていない。
【０００５】乱数系列の線形複雑度とは、その系列を生成する最小等価な線形フィードバックシフトレジスタの段数を指す。上述の周期2^n-1のＭ系列を例にとると、これはｎ段の線形フィードバックシフトレジスタで生成される最大周期の系列であるので、Ｍ系列の線形複雑度はｎである。線形複雑度が小さいと、容易に等価な乱数発生器が構成できるので、未知ビットの推測が容易で、暗号学的に安全な乱数とは言えない。
【０００６】無相関性は、例えば、乱数のビットが他の部分と独立であることを意味し、逆に相関性があると未知のビットの推測が容易となることを意味する。従来、暗号化アルゴリズムの乱数源として擬似乱数が一般に用いられてきた。しかしながら、上記した観点から擬似乱数は暗号学的に安全な乱数とは言えない。すなわち、擬似乱数は一定の算術プロセスあるいは関数の組合せから生成されるため、同じ初期条件を与えることにより同一の乱数を発生させることが可能である。従って、擬似乱数を用いた暗号は、生成法の推測も可能であり、破られやすく、秘密性の保持の点において不十分であった。
【０００７】一方、全くランダムな真性乱数に近い乱数を発生させる方法としては、自然現象、例えば放射性物質の崩壊現象等を利用した装置などがあるが、装置が大きく複雑であるという欠点を有している。従って、秘密性が高く、パーソナルコンピュータ等に容易に組み込み可能な小型の乱数生成装置の実現が要望されている。
【０００８】
【発明が解決しようとする課題】本発明はかかる点に鑑みてなされたものであり、その目的とするところは、暗号理論的に安全な２値乱数を容易に生成することが可能で、小型化に適した乱数生成装置を提供することにある。
【０００９】
【課題を解決するための手段】本発明による装置は、接合を含む半導体素子と、降伏電流が生じる程の逆バイアス電圧を接合に印加する逆バイアス印加手段と、接合を

含む電流路に生ずる雑音信号をサンプリングして得られるデジタル信号を乱数として出力するデジタル化回路と、を有する。

【0010】

【発明の実施の形態】以下に本発明の実施例を図面を参照しつつ詳細に説明する。図1は、本発明による第1の実施例である乱数生成装置の構成を概略的に示している。また、図2は図1に示した乱数生成装置の動作を説明する図であり、主要な回路ブロックの出力信号を示している。

【0011】図1において、5は雑音発生回路である。ツェナーダイオード8のｐｎ接合に抵抗器11を介して降伏が生じる程度の逆バイアス電圧を印加している。これにより、逆方向に微弱な降伏電流が流れ、ランダムな雑音電圧が発生する。このようにツェナーダイオード8を動作させることにより、ツェナ電圧を中心とした、ピーク-トゥ-ピーク（peak-to-peak）で数十～数百μＶ程度のランダムな雑音電圧出力が得られ、これを乱数の発生源としている。

【0012】具体的には、電源電圧Ｖｃｃを＋12Ｖとし、ツェナーダイオード8にはツェナ電圧が6．3Ｖと電源電圧の約1／2であるものを用いた。ツェナーダイオード8には560ｋΩの抵抗器11を介して逆バイアス電圧を印加することにより、約10μＡの逆方向電流が流れ、6．3Ｖを中心にpeak-to-peak電圧が約20μＶ、平均周波数が60～70ｋＨｚ程度の雑音電圧が発生する。（図2（ａ）参照）

雑音発生回路5で得られた雑音電圧は微弱であるので、これを増幅回路15を用いて電圧増幅する。具体的には、2段のオペアンプを用いている。この増幅回路15の電圧利得は約74ｄＢで、6．3Ｖを中心としたpeak-to-peak電圧が1Ｖ程度の増幅出力を得ることができる。（図2（ｂ）参照）

次に、増幅回路15により増幅された雑音出力は、ローパスフィルタ17に供給され高周波成分が除去される。ローパスフィルタ17のカットオフ周波数は、後述するサンプリングの周波数の数倍程度以上であればよい。ローパスフィルタ17の出力は、比較回路21に供給され、所定の基準電圧を閾値としてハイレベル、ローレベルに分けられ2値化される。

【0013】増幅雑音出力は、ツェナ電圧6．3Ｖを中心にほぼ対称であるので、ツェナ電圧を基準電圧として増幅雑音電圧の2値化を行うことができる。本実施例においては、基準電圧として非常に安定している接地電圧を用いている。すなわち、結合コンデンサ19を用い、増幅雑音出力の直流成分をカットした交流成分を比較回路21に入力している（図2（ｃ）参照）。これにより、接地電圧（0Ｖ）を閾値とした2値化を行うことができる。この構成においては、温度変化によってツェナ電圧が変化しても、直流成分が増減するのみで2値化には全く影響は生じない。従って、比較回路21の入力端には0Ｖを中心にしたpeak-to-peak電圧が1Ｖ程度の増幅雑音電圧の交流成分が入力され、接地電圧である0Ｖを閾値とした2値化が行われる。

【0014】比較回路21の出力は、レベル変換回路23に入力され、後段のサンプリング回路25の論理電圧レベルに変換される。レベル変換回路23の出力は、周期性のないランダムな矩形波である（図2（ｄ）参照）。この矩形波は、サンプリング回路25に供給される。サンプリング回路25は、入力矩形波の周波数に対してある程度低い（数分の1程度以下の）一定周波数で入力矩形波のサンプリングを行い、0及び1のビットからなる系列を得る。入力矩形波には周期性がなく、またサンプリングのタイミングは入力矩形波の周波数とは独立であるので、得られたビット系列は、0，1の各々の発生確率が等しければ、真正乱数系列であることが期待できる。

【0015】サンプリング回路25において得られた0，1からなる真正乱数の系列は、外部インタフェース（図示していない）、例えばＲＳ－232Ｃインタフェースなどを介して外部機器へ供給される。尚、サンプリング周波数は、外部機器が必要とするビットレートに設定する必要がある。上記したように、本発明によれば、半導体接合に降伏電圧程度の逆バイアス電圧を印加したときに生じる雑音を乱数の発生源とすることにより、2値の真性乱数を容易に生成することが可能である。また、上記した回路は容易にＩＣ化が可能であり、極めて小型の乱数生成装置を実現することができる。

【0016】従って、本装置を、例えばパーソナルコンピュータ等に「真性乱数発生エンジン」として組み込むことにより、デジタル署名アルゴリズムを用いた署名生成のための「真性乱数（物理乱数）」を提供することができる。すなわち、従来用いられてきた擬似乱数を用いた場合に比べはるかにセキュリティ程度の高い通信を行うことが可能となる。

【0017】図3は、本発明による第2の実施例である乱数生成装置の構成を示している。本実施例が第1の実施例と異なる点は、得られた乱数系列の0及び1の各々の発生確率が等しくなるように制御する制御部31を設けていることにある。すなわち、制御部31は、サンプリング回路25の出力を得て、この出力のうちハイレベル電圧、ローレベル電圧の各々の持続時間の累積値が互いに等しくなるように比較回路21に与える基準電圧Ｖrefを制御している。

【0018】従って、制御部31を設けて基準電圧Ｖrefを制御することにより、最終的に得られる乱数系列の0及び1の発生確率を等しくすることができ、より真性乱数に近い2値乱数系列を得ることができる。図4は、本発明による第3の実施例である乱数生成装置の構成を示している。本実施例が第1及び第2の実施例と異なる

点は、サンプリング回路２５において得られた乱数系列の０及び１の各々の発生確率が等しくなるように平滑化処理をなす平滑部３５をサンプリング回路２５の後段に設けていることにある。

【００１９】平滑化は、インバランスな０，１の系列を、x_1，x_2，x_3，…としたとき、

【００２０】

【数１】

$$y = x_1 \oplus x_2 \oplus \cdots \oplus x_n$$

【００２１】を用いて行うことができる。ここで、

【００２２】

【外１】

⊕

【００２３】は２を法とする和（排他的論理和）を表す演算である。これにより得られるｙの系列はバランス性が改善されることが示される。すなわち、x_1，x_2，x_3，…の系列中の０の発生確率をｐ，１の発生確率をｑ＝１－ｐとし、ｙに関して０の出現確率をＰ，１の出現確率をＱ＝１－Ｐとすると、ｙのインバランスは、

$P-Q=(p-q)^n$

で与えられる。ここで、ｎは平滑化におけるブロックサイズである。ｎを大きくとれば、インバランス性は指数関数的に小さくなる。

【００２４】尚、図４においては平滑部３５をハードウエアの構成として説明したが、実際はコンピュータのソフトウエアで容易に実現可能であり、コンピュータ側で必要な程度（ブロックの大きさ）で行えば十分である。以上の処理を行うことによって、より真正乱数に近い０，１の系列を得ることができる。尚、上記実施例においては、雑音発生源としてツェナーダイオードを用いた場合を例に説明したが、これに限らず、例えば異種導電型の半導体接合を用い、その降伏電流を雑音発生源として用いてもよい。

【００２５】

【発明の効果】以上詳細に説明したように、本発明によれば、半導体接合の降伏電流を雑音発生源として用いることにより、暗号理論的に安全な２値乱数を容易に生成することが可能で、かつ小型化に適した乱数生成装置を実現することができる。

【図面の簡単な説明】

【図１】本発明による第１の実施例である乱数生成装置の構成を示す図である。

【図２】図１に示した乱数生成装置の動作を説明する図である。

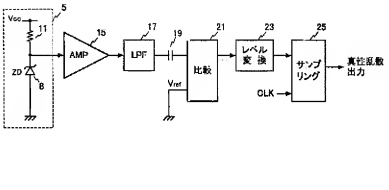
【図３】本発明による第２の実施例である乱数生成装置の構成を示す図である。

【図４】本発明による第３の実施例である乱数生成装置の構成を示す図である。

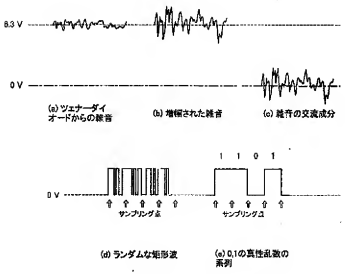
【主要部分の符号の説明】

５　雑音発生回路
８　ツェナーダイオード
１１　抵抗器
１５　増幅回路
１７　ローパスフィルタ
２１　比較回路
２３　レベル変換回路
２５　サンプリング回路
３１　制御部
３５　平滑部

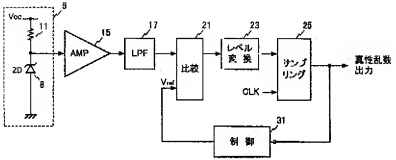
【図１】



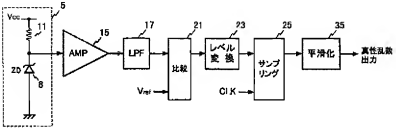
【図2】


8.3 V
0 V
(a) ツェナーダイオードからの雑音
(b) 増幅された雑音
(c) 雑音の交流成分
1 1 0 1
0 V
サンプリング a
サンプリング b
(d) ランダムな矩形波
(e) 0,1の真性乱数の系列

【図3】


Vcc
5
11
AMP
15
LPF
17
比較
21
レベル変換
23
サンプリング
25
真性乱数出力
ZD
8
Vref
CLK
制御
31

【図4】


Vcc
5
11
AMP
15
LPF
17
比較
21
レベル変換
23
サンプリング
25
平滑化
35
真性乱数出力
ZD
8
Vref
CLK